SECTION II –STATEMENT OF WORK

1.0 GENERAL

1.1 BACKGROUND

On January 9, 2004 President Bush initiated a three (3) year Safety, Health and Return-to-Employment. (SHARE) Initiative, which directed federal agencies including the Department of Homeland Security (DHS) to reduce workplace injuries and illness, lost time and lost production day rates, and improve the workers' compensation claims reporting process for work injuries and illnesses.

Since the implementation of this initiative in 2004, several federal agencies and departments have significantly reduced their injury and illness and lost time case rates as well as improved the timely reporting process of work and illness claims. At the end of Fiscal Year (FY) 2005, the initiative's second year, the Federal Government as a whole had reduced injury and illness cases by 5.5%, lost time cases by 2.6%, and increased timely workers' compensation claims submission by 70.9% (Baseline FY 2003).

In October 2006 President Bush announced the extension of the SHARE Initiative for all federal agencies through FY 2009 and revised the goals for timely claims processing and lost production days rate. The extension of the Initiative is the President's commitment to improving the workplace safety and health conditions for all federal employees while reducing the financial cost to the American taxpayers for disability claims.

Recently the Obama Administration established a 4-year Protecting Our Workers and Ensuring Reemployment (POWER) Initiative, covering fiscal years 2011 through 2014. The POWER Initiative extends prior workplace safety and health efforts of the Federal Government by setting more aggressive performance targets, encouraging the collection and analysis of data on the causes and consequences of frequent or severe injury and illness, and prioritizing safety and health management programs that have proven effective in the past.

To continue to support the President's POWER Initiative, TSA needs to ensure that the POWER Initiative goals and Performance targets are achieved or exceeded in each category by the end of each FY. To accomplish these goals, Workers' Compensation cases need to be medically managed with continued

follow through until resolution has been reached on each case. Periodic Roll workers' compensation cases need to be evaluated to obtain resolutions that lead to employees returning to duty in some capacity, i.e., receiving reassignment within the TSA organization, or another government agency, or being placed into the Department of Labor's Vocational Rehabilitation Program to receive commercial employment services. For this cause, the Workers' Compensation Program (WCP) office was established.

The WCP provides the majority of its services to Transportation Security Officers (TSOs), located at the various airports within the U.S and its territories. Out of a TSA work force of 60,000 full and part time employees, approximately 47,000 are full time equivalent security officers, who provide security for airports and other transportation modes. The job requirement for Transportation Security Officers include the ability to repeatedly lift and carry items weighing up to 70 pounds, walking up to two miles daily, and the ability to stand for prolonged periods of time. As a result of the strenuous job requirements, officers have experienced injuries at a rate that was approaching 30 percent of the officer workforce, which has proved to be financially costly, as well as a potential security risk, due to lack of security coverage available to perform security task associated with security screening operations.

1.2 SCOPE

The Contractor shall provide a full range of Workers' Compensation, Medical Case Manager (MCM) Services to support an approximate 1,700 open workers' compensation cases. In addition, **the TSA expects an annual case load of approximately 5,000 new First Report of Injury (FROI). MCM Services are required throughout the United States in all 50 States, the District of Columbia, and U.S. Territories including Puerto Rico, U.S. Virgin Island, Guam, Northern Mariana Islands and American Samoa.**

The Contractor shall provide a toll free Injury Reporting Hotline, 24 hours a day, seven days a week, to capture and input data from the FROI, and provide live coverage to receive calls and input data received from the Injury Reporting Hotline into a case management database. The scope of this requirement is for MCM Services with an ancillary, already functioning Information Technology (IT) solution, to enable Nurses to execute case management processes, and allow the electronic case management activities to be performed at local airports by TSA HR staff.

The Contractor shall provide MCM Services encompassing: (1) Injury Care Support Services; (2) Medical Case Management Services; and (3) An enabling IT Solution. These three requirements are described in detail within the Statement of Work (SOW) Section 2.0.

The Contractor shall be required to proactively manage cases of all durations, including long-term (Periodic Roll) claims, from the FROI through a successful Return-to-Work or case resolution.

The Contractor shall manage cases to support the Workers Compensation Goals and comply with applicable guidance, including the POWER Initiative.

1.3 OBJECTIVE

The objective of this requirement is for the TSA to obtain a qualified Contractor that shall provide medical case management services inclusive of a functioning IT solution to assist TSA in the timely and successful return of its employees to the workforce.

1.4 APPLICABLE REQUIREMENT

1.4.1 FEDERAL REQUIREMENTS

- ATSA PL 107-71, Aviation and Transportation Security Act, 49 USC 40101 http://www.tsa.gov/assets/pdf/Aviation_and_Transportation_Security_Act_ATSA_Public_Law_107_1771.pdf
- Federal Employees' Compensation Act (FECA), 5 U.S.C. §§ 8101 *et seq.* http://www.dol.gov/owcp/dfec/regs/statutes/feca.htm
- 20 CFR Part 10 http://www.gpo.gov/fdsys/pkg/CFR-2007-title20-vol1/pdf/CFR-2007-title20-vol1.pdf
- Injury Compensation for Federal Employees, Office of Workers' Compensation Programs (OWCP) publication CA-810 http://www.dol.gov/owcp/dfec/regs/compliance/DFECfolio/CA-810.pdf
- Privacy Act of 1974 (5 USC 552a) Public Information http://www.opm.gov/feddata/USC552a.txt
- TSA Management Directive (MD): MD 1100.00-6. Workers' Compensation Program and Handbook
- TSA Office of the Chief Information Officer, Systems Development Life Cycle (SDLC) 2.0.4, July 2005
- DHS TSA Office of the Chief Information Officer Systems, Life Cycle (SLC) Guidance Document, version 0.9, dated December 14, 2007

1.4.2 APPLICABLE DOCUMENTS

- 5 United States Code (USC) §§ 8101 - 8193 http://www.dol.gov/owcp/dfec/regs/statutes/feca.htm
- 20 Code of Federal Regulations (CFR) Part 10 http://www.gpo.gov/fdsys/pkg/CFR-2007-title20-vol1/pdf/CFR-2007-title20-vol1.pdf
- Department of Labor Office of Workers' Compensation Programs (OWCP) requirements (Information is available at http://www.dol.gov)
- National Archive and Record Act regarding record retention, 36 CFR 1220,14 http://www.archives.gov/about/regulations/part-1220.html
- Privacy Act, 5 USC § 552a http://www.opm.gov/feddata/USC552a.txt

- DHS MD 4300.1, Information Technology Systems Security
- DHS 4300A, Sensitive Systems Handbook
- TSA MD 1400.3, Information Technology Security Policy (ITSP) Handbook
- TSA MD 11056.1, Sensitive Security Information (SSI)
- All applicable DHS and TSA Management Directives, as deemed necessary
- NIST SP 800-53, Rev 3, Recommended Security Controls for Federal Information Systems

1.4.3 TSA is required to achieve or exceed the SHARE/POWER Initiative goals by implementing the following guidelines and procedures that support the Initiative.

The SHARE / POWER Initiative Goals are to:

a. Reduce the total case rates for injuries and illness by at least 3% per FY
b. Reduce the case rates for lost time injuries and illness by at least 3% per FY
c. Reduce the rates of lost production days due to injuries and illnesses by at least 1% per FY
d. Increase the timely filing of injury and illness notices by at least 5% per FY
e. Analyze lost time injury and illness data
f. Increase timely filing of wage-loss claims by at least 1%
g. Speeding employees' return to work in cases of serious injury or illness

1.4.4 TSA is required to follow all applicable regulations and statues under FECA.

1.4.5 TSA is required to meet legislative requirements of the Aviation and Transportation Security Act (ATSA), Pub. Law 107-71 (November 19, 2001), and comply with applicable statutes, regulations, and requirements of the Department of Labor (DOL) Office of Workers' Compensation Programs (OWCP) by implementing guidelines and procedures that support the regulations, requirements, and statutes.

1.4.6 TSA is required to comply with Department of Homeland Security FISMA and TSA's security Certification and Accreditation (C&A) requirements and federal privacy regulations, including the submission of all required security documentation.

2.0 THE MEDICAL CASE MANAGEMENT STAFF REQUIREMENTS/TASKS

2.1 TASK ONE. MEDICAL CASE MANAGERS

2.1.1 The Contractor shall provide Medical Case Managers (MCM) as certified/licensed Registered Nurses (RN) within the respective state(s) or maintain a respective Nurse Licensure Compact that enables multistate licensure. **Qualified MCMs shall provide oversight to injured/ill employees throughout the medical treatment process.** The MCM shall facilitate or advocate for medical options and services to assist in the recovery process of TSA employees who have suffered a work related injury. The MCM shall serve as the liaison between the TSA employee, and the medical community, the TSA Headquarters Workers' Compensation Program Office (WCPO), and the field Workers' Compensation Coordinators (WCC). The MCM shall provide medical advice, guidance, and support as appropriate.

NOTE: The Contractor shall provide at least one MCM that holds a valid California Nursing License.

2.1.2 The MCMs shall adhere to the following standards and provide and/or perform the following functions:

2.1.3 The MCMs shall make initial contact with the injured TSA employees within 24 hours of the date of the reported injury to the Injury Reporting Hotline. The initial acceptable means of contact shall be telephonic only. The initial contact must consist of the following, and other processes, that the MCMs deem appropriate or necessary to support the process:

- **2.1.3.1** Provide a personal introduction
- **2.1.3.2** Provide contact information
- **2.1.3.3** Start establishing a rapport with the injured TSA employee
- **2.1.3.4** Gather information and history of injury in anatomical location
- **2.1.3.5** Obtain treating physician(s) information for follow-up
- **2.1.3.6** Assist in scheduling diagnostic testing when appropriate
- **2.1.3.7** Continue follow-up through case closure/resolution
- **2.1.3.8** Address injured employees concerns when appropriate

2.1.4 The MCMs shall notify the WCC by telephone within 48 hours of the date of the reported injury or illness. The contact process should consist of the following and other processes the MCMs deem appropriate or necessary to support the process:

2.1.4.1 Provide a personal introduction
2.1.4.2 Start establishing a rapport
2.1.4.3 Provide contact information
2.1.4.4 Establish a plan of action with the TSA Workers' Compensation representative
2.1.4.5 Continue follow-up through case closure/resolution.

2.1.5 The MCMs shall make contact with the TSA employee's medical providers(s) office(s) within 48 hours of the date of the reported injury or illness if necessary. The contact should consist of the following and other processes the MCMs deem appropriate or necessary to support the process:

2.1.5.1 Provide a personal introduction
2.1.5.2 Provide contact information
2.1.5.3 Establish a rapport with the physician's office personnel
2.1.5.4 Learn of the treatment plan
2.1.5.5 Facilitate diagnostic testing as required.
2.1.5.6 Continue documented follow-up through case closure/resolution.

2.1.6 The MCMs shall follow up with the injured/ ill TSA employee at minimum 30, 60, and 90 day intervals until resolution (Additional contact may be required depending upon complexity of the injury/illness). Each follow up contact shall be documented in medical case management database.

2.1.7 The MCMs shall follow up with the TSA WCC at a minimum of 30, 60, 90 day intervals until resolution (Additional contact may be required and is driven by the complexity of the case). Each follow up shall be documented in Medical case management database.

2.1.8 The MCMs shall follow up with the injured or ill TSA employee's medical provider(s) at a minimum of 30, 60, 90 day intervals until resolution if necessary (Additional contact may be required and is driven by the complexity of the injury/illness). Each follow up shall be documented in medical case management database.

2.1.9 The MCMs shall assess the TSA employee's injury/illness records. The assessment includes reviewing medical documentation, evaluating the TSA employee's progression to recovery, employee participation and the need for specialized testing (i.e. MRI, CT scan, physical therapy, work hardening...).

2.1.10 The MCMs shall assist TSA by validating the medical treatment plans of injured/ ill TSA employees. The validation process includes confirming that the medical treatment plans are within industry standards for the type of injury/ illness and that they are suitable for the expected recovery. The MCMs shall inform the TSA WCC if the medical treatment plans are not appropriate for the type of injury or illness.

2.1.11 **The MCMs shall assist the TSA employees in coordinating referrals from treating physician to medical facilities for diagnostic and testing services, as appropriate, for care and treatment.** In addition, the MCM shall notify TSA employees of scheduled appointment dates and times as well as provide the TSA WCC of the medical results within 24 hours of receipt of results.

2.1.12 The MCMs shall assist in the Limited Duty Assignment process by providing clarity to medical restrictions and following up with the employees after returning to work. This follow up shall be

in two (2) week intervals until the employee returns to their pre-injury state.

2.1.13 **The MCM shall assist TSA in return to work efforts by reviewing Periodic Roll and long-term limited duty cases.** The MCM shall assess all of the medical documentation for that case and request updated medical documentation when appropriate. The MCM shall assist with assessing individual's opportunities to return to work based upon their medical progress and recovery. The MCM shall follow up on these cases at a minimum of 30, 60, 90 day intervals until resolution (Additional reviews may be required and is driven by the complexity of the case). A TSA WCC or a TSA WCPO will provide the Contractor with the Periodic roll workers' compensation and long term limited duty claims to be distributed to the MCM to execute into the Workers' Compensation Medical Case Management program.

2.1.14 The MCM shall ensure the safe, professional, and efficient administration of all aspects of assessment process, and medical oversight/management. This shall include, but is not limited to, ensuring that all assessments are being conducted appropriately.

2.1.15 The MCM shall orient Human Resources Specialists (and other TSA Personnel as appropriate) to the TSA National Medical Case Management Program, including the use of medical case management software, and assist TSA HQ in providing guidance on the use of TSA Workers' Compensation Documentation (Rights & Responsibilities Documents), and Workers' Compensation Case Management Best Practices.

2.1.16 The MCM shall assist with developing and implementation of supervisor and manager workers' compensation training efforts at local airports.

2.1.17 MCM shall elevate all technical FECA related issues directly to the respective WC Program Office Area Specialist.

2.1.18 The MCM shall provide smooth transition of documents and open communication with TSA HR Specialist and/or HQ-WC Team, regarding medical updates obtained from doctor offices, employee statements, and doctor office personnel comments, and/or any evidence related to the injury claim.

2.1.19 The MCM shall review medical documentation for Scheduled Award claims specifically the medical and physician's test results and conclusions, to determine if the impairment rating is accurate, and if not, provide objective rationale for why it is not so that the information can be presented to the HR Specialist, and ultimately to OWCP.

2.1.20 The MCM shall continually provide case management to a point of Case Closure resulting in one of the following activities:

- 2.1.20.1 A medical resolution of the work-related injury,
- 2.1.20.2 Claimant reaching Maximum Medical Improvement (not preventative limitations)
- 2.1.20.3 TSA HR Specialist declines further services
- 2.1.20.4 OWCP placement in Vocational Rehabilitation program
- 2.1.20.5 An assignment to OWCP Direct Placement
- 2.1.20.6 Claims Disallowed by OWCP

2.1.21 The MCM and/or MRP shall conduct or participate in monthly telephonic training pertinent medical issues to WCC's and Headquarter Workers' Compensation Program personnel.

2.1.22 The MCM shall monitor prescription drug usage through appropriate Pharmacy Benefits Management (PBM) Network. Monitor and track case status for each case managed through to resolution.

2.1.23 The MCM shall be an active resource in TSA's Continuity of Operations Plan (COOP) preparations and processes. Provide related program support when called upon.

2.1.24 The MCM shall develop case medical case management strategies on complex cases to include guidance and recommendations from the HQ-WCP. Provide periodic program reviews with the HQ-WCP for the purposes of identifying all areas of opportunities for overall program refinement.

2.1.25 The MCM shall establish the nurse intervention/case management services from the date of injury or notification of the injury. If and when OWCP assigns one of their internal nurses to the case the MCM shall yield to the OWCP nurse and cooperate with the OWCP nurse as needed. When OWCP Nurse closes their file the MCM will reevaluate the case for appropriateness in additional management efforts.

2.2 **TASK TWO. THE MEDICAL REVIEW PHYSICIAN (MRP).** The Contractor shall provide a (Licensed)MRP that shall provide the following:

2.2.1 The MRP shall review complex cases, as referred by the TSA HR Specialist, and/or HQ-WC Team.

2.2.2 The MRP shall document all cases exceeding Estimated Disability Duration (EDD) periods as established by industry standards, i.e. Medical Disability Advisers (MDA) or similar program. The MRP shall prepare a report on each case that exceeds EDD. This report shall contain justification for the extended disability period with recommendations for continued case management activities leading to case resolution or best possible outcome.

2.2.3 The MRP shall communicate in writing with the injured employees' treating physician on complex medical issues that need clarification and may be impacting return to work opportunities.

2.2.4 Upon authorization from the HQ- WC Team the MRP may communicate in writing with the OWCP claims examiner and/or district medical advisors on complex medical issues impacting return to work and long-term medical accommodation issues.

2.2.5 Develop medical discussion topics for monthly informational teleconferences with agency Workers Compensation Coordinators and HQ-WC team members.

2.2.6 The MRP shall assist TSA by validating the medical treatment plans and mechanism of injury issues in complex claims.

2.3 **TASK THREE. INJURY CARE SUPPORT SERVICES**

2.3.1 **The Contractor shall provide a staffed toll free Injury Reporting Hotline operating 24 hours per day, seven days per week to receive all First Report of Injury calls from all TSA installations globally.**

2.3.2 The Contractor shall provide 24 hour per day, seven days per week telephonic support to input data received from the FROI into the medical case management database and alert the appropriate MCM.

2.3.3 All Injury Care Support personnel receiving or responding to TSA callers shall be trained in customer service and knowledgeable and familiar with the TSA Workers' Compensation

program goals and objectives.

2.3.4 All Injury Care Support personnel shall maintain professional, accurate, and timely customer service in all dealings; for example: Understand employee issues; follow up on employee issues; resolve issues that may be preventing an employee from returning to duty; assess underlying employee needs.

2.3.5 All Injury Care Support personnel shall be able to communicate through toll-free phone lines, fax machine, e-mail and the United States Postal Service as well as having the communications capability to receive or send information to TSA sites located outside the continental United States (regardless of time zone).

2.4 TASK FOUR. CONTRACT PROJECT MANAGEMENT

2.4.1 The Contractor shall utilize the case management database to centrally manage, store, document and report all case management activities from the initial injury notification up to and including case resolution / closure.

2.4.2 The Contractor shall participate in weekly program status meetings with the WCP during contract transition. Thereafter, status meeting will be held on bi-weekly bases unless otherwise directed by WCP.

2.4.3 The Contractor shall provide program activity and status reports on a, daily, weekly, monthly, quarterly, semi-annual and annual bases. The WCP shall at a minimum have the following reporting topics:

2.4.3.1 Claims Activity Report (a report defining new and active claims)

2.4.3.2 Periodic Roll (PR) Medical Management Report (a report defining all PR cases and current medical status to include medical treatment plan as defined by MCM, MRP and HQ WCP)

2.4.3.3 Catastrophic Event Report (a report listing FROI's as noted in item 2.4.8 below)

2.4.3.4 Supervisor to MCM Timely Notification Report (a report of tracking supervisor to Hotline notification)

2.4.3.5 Medical Management Report (Medical status report). A Medical Status Report is a report containing the most recent medical status of each claim in the program. Status meaning; total disability, fit for limited duty, fit for regular duty and etc.

2.4.3.6 Limited Duty not Available Report (Reporting indicating an employee with medical restrictions that can't be accommodated)

2.4.3.7 Limited Duty Report (A report listing employees on limited duty)

2.4.3.8 Monthly Case Management Report (Detailed monthly case management status report)

2.4.3.9 Periodic Roll Report (A detailed account of claims on the periodic roll)

2.4.3.10 Periodic Roll Case Summary Report (A summary of cases on the periodic roll)

2.4.3.11 After Action (PR) report (A report of all closed PR cases)

2.4.4 The Contractor shall provide an annual Quality Assurance Report to the Workers' Compensation Program Office (WCP). The Quality Assurance Report shall include, but not be limited to the following:

2.4.4.1 Employee screening regarding the recruitment, hiring and retaining qualified employees

2.4.4.2 Staff training regarding initial and periodic training to include TSA mandated training

2.4.4.3 MCM Program Operating Policies and Procedures in regards to ensuring that task order personnel are in compliance with program policies and procedures.

2.4.4.4. Responsiveness of IT System: Track to ensure timely notification of potential WC claims activity from initial notification to MCM being made aware of potential claim.

2.4.4.5 IT System Availability: Percentage of time the IT system is available for case management activities.

2.4.5 The Contractor shall provide a tool to monitor Customer Satisfaction of Nurses interaction with injured employees, HR and Management staff members.

2.4.6 The Contractor shall provide TSA with recommendations to improve overall quality, ease of use, efficiency and effectiveness of the Worker's Compensation Medical Case Management program.

2.4.7 The Contractor shall deliver a bi-weekly report that details actual progress against the performance goals that follow. Report formatting is subject to TSA approval. The WCP will have the option of scaling back the report to a monthly deliverable as the program matures.

2.4.8 Contractor shall have a MRP and MCM available after hours and on weekends to support TSA if a media worthy or catastrophic event should arise called in as a FROI. A catastrophic report isdefined as follows:

2.4.8.1 By incident involving multiple exposures.
2.4.8.2 Any acts of physical violence.
2.4.8.3 Multiply injuries arising out of the same event.
2.4.8.4 Potentially newsworthy events.
2.4.8.5 A serious or life threatening injury.
2.4.8.6 Injury involving Emergency Medical Transportation to Emergency room.
2.4.8.7 Stress related incidents.
2.4.8.8 The Contractor shall immediately contact the HQ-WCP Program Manager of all catastrophic events as defined above.

2.4.9 The Contractor shall develop case management strategies on complex cases to include guidance and recommendations from the HQ-WCP. The Contractor shall also engage in periodic program reviews with the HQ-WCP for the purposes of identifying all areas of opportunities including all refinement possibilities.

2.4.10 The Contractor shall make ongoing recommendations to TSA on ways to improve the assessment process.

2.4.11 The Contractor shall be an active resource in TSA's Continuity of Operations Plan (COOP) preparations and processes and provide program support when called upon.

2.5 TASK FIVE. MCM SERVICES/INFORMATION TECHNOLOGY (IT) SOLUTION (Project Management Support Services)

2.5.1 The Contractor shall provide a total solution that allows Nurses to execute case management processes, and allows the electronic case management activities to be performed at local airports by TSA HR staff. **TSA is not requesting the development of an IT solution.** The functioning IT solution is ancillary to the delivery of the services and shall include a medical case management database that will assist in managing workers compensation claims throughout the claims entire lifecycle. The medical case database shall include a robust report module to enhance the overall effectiveness of the Workers' Compensation Program Office within OHC while assuring TSA employees, injured in the performance of duty, receive optimal treatment while recovering from job related injuries and illnesses.

The already functioning database shall have at least the following capabilities:

- create individual electronic case files, capturing all case information, including scanned documentation, and being a repository for case management files;
- twice daily updates;
- physically separated from all other government agencies or client infrastructures;
- provide national secured access "In Read only" format to TSA Workers' Compensation HQ group (approximately 8 HQ users);
- TSA HR field site representatives shall have local access based on their current area(s) of responsibility (approximately 150 field users);
- provide real-time detail activities for the case file information and reports of the current medical status of injured employees;

capability to identify duplicate claims; and identify each individual case file with a unique system generated numerical/alpha claim identifier.

- training for TSA users on the IT solution application that will be used to manage workers' compensation cases. This training will be delivered in a format consistent with TSA's learning management system. The Contractor shall conduct future recurring training for its users, as needed.
- provide fixed and ad hoc reporting capabilities.
- accessible via a web-based Internet interface with secure logon capabilities for multiple users and capabilities to allow multiple users view the same document(s) simultaneously.
- restricted to classes of authorized users ("roles") having the authority to view specific pages, update specific pages and delete specific pages
- capability to restrict critical functions (e.g., adding/deleting users, removing cases) only to Administrators.
- tracks changes, updates, and modifications to Nurse Case Management components and business rules over its lifespan.
- set and view flags that show various case statuses for each case.
- assign unique OWCP case numbers for each new injury.
- case attachments to allow forms, letters, faxes, emails, medical results, etc., to be stored with each case and be viewable and printable.
- audit logging that tracks username, date and time stamping of every transaction associated with case access, modification, and system changes.
- dashboard view of cases assigned to the user (to include but not limited to indicators, status, tasks, etc.).
- a medical provider database to allow the entry, edit and deletion of provider information (Each entry to contain the Name, Specialty, Address, Phone, (optional) email and (optional) Fax Number of each provider.]
- flag all cases that happen between the hours of 7 PM and 7 AM Eastern Standard Time (EST) in addition to weekends and holidays.
- flag all catastrophic cases.
- close cases and be reopened at a later time.
- send and receive information via secured fax and e-mail (These will be two different fax numbers and e-mail addresses).
- set alert indicators ("ticklers") for case follow-up.
- an internal table of locations with each location assigned a region and a case manager (name and e-mail address) and a time zone.
- provide access to, EDD, International Classification of Disease, 9th Revision Codes, Current Procedural Terminology Codes, Job Position Industry Standards, levels and descriptions and other relative software applications.
- internal communication capabilities.
- performance goals or outcomes from the technical requirements are:
    1. Responsiveness of Medical Case Managers. This is defined as percentage of time an injured employee is contacted by MCM within the required 24 hour time period.
    2. Medical Case Manager Contractor Effectiveness. This is defined as percentage of cases returning to work within industry standard EDD periods.

3. At least 98% IT System responsiveness. This is defined as the percentage of time to provide automated First Report of Injury (FROI) notification to Medical Case Managers (MCM) and Worker's Compensation Coordinator (WCC) within 5 minutes.
4. At least 98% IT System uptime. This is defined as the percentage of time the system will be available for case management activities by system users, excluding IT system routine maintenance.

System responsiveness and uptime will be tracked by TSA via real time and through Deliverable No. 9 (Operational Performance Report). Responsiveness and uptime that falls below 98% will be considered a performance issue.

3.0 PROJECT MANAGER
(See Tasks under Section 2.4)

The Contractor shall provide a Project Manager who shall be responsible for all Contractor work performed under this SOW. The Project Manager shall be a single point of contact for the Contracting Officer, the Contracting Officer Technical Representative (COTR), and the HQ-WCP Program Manager. The Name of the Project Manager, and the name of any alternative(s) who shall act for the Contractor in the absence of the Project Manager, shall be provided to the Government as part of the Contractor's proposal. The Project Manager is further designated as Key by the Government. During any absence of the Project Manager, only one alternate shall have full authority to act for the Contractor on all matters relating to work performed under this task order. The Project Manager and all designated alternatives shall be able to read, write, speak and understand English. Additionally, the Contractor shall not replace the Project Manager without prior acknowledgement from the Contracting Officer.

3.1 The Project Manager shall be available to the HQ-WCP Program Manager and COTR via telephone between the hours of 8am and 5pm EST, Monday through Friday, and shall respond to a request for discussion or resolution of technical problems within the time requested.

4.0 POST AWARD CONFERENCE

The Government shall conduct a Post Award Conference. The purpose of the Post Award Conference is to discuss the task order and to clarify and establish roles and responsibilities under the task order. The Conference will be chaired by the Contracting Officer with the attendance of the COTR and Contractor

and other personnel deemed necessary by the Contracting Officer. The Conference will be held within fifteen calendar days after task order award. The Conference will be held at the Government's designated facility or via teleconference.

The Contractor's Draft Project Plan shall be submitted 10 calendar days after award of task order.

4.1 FINAL PROJECT PLAN

The Contractor shall deliver the Final Project Plan to the COTR not later than thirty calendar days after award of the task order.

4.2 BUSINESS CONTINUITY PLAN

The Contractor shall prepare and submit a Business Continuity Plan (BCP) to the Government. The BCP Plan shall be due 30 calendar days after the date of award, and will be updated on an annual basis. The BCP shall document Contractor plans and procedures to maintain support during an emergency, including natural disasters and acts of terrorism. The BCP, at a minimum, shall include the following:

-A description of the Contractor's emergency management procedure and policy

-A description of how the Contractor will account for their employees during an emergency

-How the Contractor will communicate with the Government during emergencies

-A list of primary and alternative Contractor points of contact, each with primary and alternate:

Telephone numbers

E-Mail addresses

4.2.1 The Contractor's BCPs shall be activated immediately after determining that an emergency has occurred, and shall be operational within one (1) hour of activation or as directed by the Government, and shall be sustainable until the emergency situation is resolved and normal conditions are restored or the task order is terminated, whichever comes first. In case of a life threatening emergency, the COTR shall immediately make contact with the Contractor Project Manager to ascertain the status of any Contractor personnel who were located in Government controlled space affected by

the emergency. When any disruption of normal, daily operations occur, the Contractor Project Manager and the HQ-WCP Program Manager or COTR shall promptly open an effective means of communications and verify.**4.2.2** The Government and Contractor Project Manager shall make use of the resources and tools available to continue contracted functions to the maximum extent possible under emergency circumstances. Contractors shall obtain approval from the Contracting Officer prior to incurring costs over those allowed for under the terms of this task order. Regardless of task order type, and of work location, the Contractors performing work in support of authorized tasks within the scope of their task order charge those hours accurately in accordance with the terms of the task order.

4.3 SECTION 508 COMPLIANCE

Electronic and Information Technology to Accommodate users with Disabilities (Section 508 of the Rehabilitation Act)

Section 508 of the Rehabilitation Act prohibits federal agencies from procuring, developing, maintaining, or using electronic and information technology (EIT) that is inaccessible to people with disabilities. The applicable standards in Section 508 of the Rehabilitation Act, as amended, shall apply to this contract and any items, or services covered by or provided in connection with this requirement. The Contractor shall provide items and services that comply with Section 508 requirements and the Electronic and Information Accessibility Standards at 36 CFR Part 1194.

4.3.1 Section 508 Applicable EIT Accessibility Standards

36 CFR 1194.21 Software Applications and Operating Systems, applies to all EIT software applications and operating systems procured or developed under this work statement including but not limited to GOTS and COTS software. In addition, this standard is to be applied to Web-based applications when needed to fulfill the functional performance criteria. This standard also applies to some Web based applications as described within 36 CFR 1194.22.

36 CFR 1194.22 Web-based Intranet and Internet Information and Applications, applies to all Web-based deliverables, including documentation and reports procured or developed under this work statement. When any Web application uses a dynamic (non-static) interface, embeds custom user control(s), embeds video or multimedia, uses proprietary or technical approaches such as, but not limited to, Flash or Asynchronous Javascript and XML (AJAX) then 1194.21 Software standards also apply to fulfill functional performance criteria.

36 CFR 1194.24 Video and Multimedia Products, applies to all video and multimedia products that are procured or developed under this work statement. Any video or multimedia presentation shall also comply with the software standards (1194.21) when the presentation is through the use of a Web or Software application interface having user controls available.

36 CFR 1194.31 Functional Performance Criteria, applies to all EIT deliverables regardless of delivery method. All EIT deliverable shall use technical standards, regardless of technology, to fulfill the functional performance criteria.

36 CFR 1194.41 Information Documentation and Support, applies to all documents, reports, as well as help and support services. To ensure that documents and reports fulfill the required 1194.31 Functional Performance Criteria, they shall comply with the technical standard associated with Web-based Intranet and Internet Information and Applications at a minimum. In addition, any help or support provided in this work statement that offer telephone support, such as, but not limited to, a help desk shall have the ability to transmit and receive messages using TTY.

4.3.2 Section 508 Applicable Exceptions

Exceptions for this work statement have been determined by DHS and only the exceptions described herein may be applied. Any request for additional exceptions shall be sent to the COTR and determination will be made in accordance with DHS MD 4010.2. DHS has identified the following exceptions that may apply: 36 CFR 1194.3(b) Incidental to Contract, all EIT that is exclusively owned and used by the contractor to fulfill this work statement does not require compliance with Section 508. This exception does not apply to any EIT deliverable, service or item that will be used by any Federal employee(s) or member(s) of the public. This exception only applies to those contractors assigned to fulfill the obligations of this work statement and for the purposes of this requirement, are not considered members of the public.

4.3.3 Section 508 Compliance Requirements

36 CFR 1194.2(b) (COTS/GOTS products), When procuring a product, each agency shall procure products which comply with the provisions in this part when such products are available in the commercial marketplace or when such products are developed in response to a Government solicitation. Agencies cannot claim a product as a whole is not commercially available because no product in the marketplace meets all the standards. If products are commercially available that meets some but not all of the standards, the agency must procure the product that best meets the standards. When applying this standard, all procurements of EIT shall have documentation of market research that identify a list of products or services that first meet the agency business needs, and from that list of products or services, an analysis that the selected product met more of the accessibility requirements than the non-selected products as required by FAR 39.2. Any selection of a product or service that meets less accessibility standards due to a significant difficulty or expense shall only be permitted under an undue burden claim and requires authorization from the DHS Office of Accessible Systems and Technology (OAST) in accordance with DHS MD 4010.2.

4.4 ACCESS TO UNCLASSIFIED FACILITIES, IT RESOURCES, AND SENSITIVE INFORMATION

The assurance of the security of unclassified facilities, Information Technology (IT) resources, and sensitive information during the acquisition process and contract performance are essential to the DHS mission. DHS Management Directive (MD) 11042.1 Safeguarding Sensitive but Unclassified (For Official Use Only) Information, describes how contractors must handle sensitive but unclassified information. DHS MD 4300.1 Information Technology Systems Security and the DHS Sensitive Systems Handbook prescribe policies and procedures on security for IT resources. Contractors shall comply with these policies and procedures, any replacement publications, or any other current or future DHS policies and procedures covering contractors specifically for all Task Orders that require access to DHS facilities, IT resources or sensitive information. Contractors shall not use or redistribute any DHS information processed, stored, or transmitted by the contractor except as specified in the task order.

4.4.1 Security Review

The Government may elect to conduct periodic reviews to ensure that the security requirements contained in this task order are being implemented and enforced. The Contractor shall afford DHS, including the organization of the DHS Office of the Chief Information Officer, the Office of the Inspector General, authorized Contracting Officer's Technical Representative (COTR), and other government oversight organizations, access to the Contractor's facilities, installations, operations, documentation, databases and personnel used in the performance of this task order. The Contractor will contact the DHS Chief Information Security Officer to coordinate and participate in the review and inspection activity of government oversight organizations external to the DHS. Access shall be provided to the extent necessary for the government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability and confidentiality of DHS data or the function of computer systems operated on behalf of DHS, and to preserve evidence of computer crime.

4.5 ARCHITECTUAL COMPLIANCE

4.5.1 DHS Enterprise Architecture Compliance

All solutions and services shall meet DHS Enterprise Architecture policies, standards, and procedures. Specifically, the contractor shall comply with the following Homeland Security Enterprise Architecture (HLS EA) requirements:

4.5.1.1 All developed solutions and requirements shall be compliant with the HLS EA.

4.5.1.2 All IT hardware or software shall be compliant with the HLS EA Technical Reference Model (TRM) Standards and Products Profile.

4.5.1.3 All data assets, information exchanges and data standards, whether adopted or developed, shall be submitted to the DHS Enterprise Data Management Office (EDMO) for review and insertion into the DHS Data Reference Model.

4.5.1.4 In compliance with Office of Management and Budget (OMB) mandates, all network hardware shall be IPv6 compatible without modification, upgrade, or replacement.

4.5.2 TSA Architectural Compliance

The Contractor shall prepare and submit a Data Management Plan (DMP) to the Government. The DMP shall be due 60 calendar days within the start of task order services. All solutions and designs shall be approved by the Enterprise Architecture Division (EAD) prior to being implemented through the SELC Solution Engineering Review (SER), Preliminary Design Review (PDR) and Critical Design Review (CDR) stage gates. All implementations shall be done per the approved solution/design without deviation. Any solution or design changes identified during subsequent SELC phases, including testing, implementation and deployment, must first receive EAD review and approval. All solution and design artifacts (e.g. FRDs, SDDs, and SSPs) are to be placed in the specified EAD repository.

4.6 Controls

The Contractor shall comply with Department of Homeland Security (DHS) and Transportation Security Administration (TSA) technical, management and operational security controls to ensure that the Government's security requirements are met. These controls are described in DHS PD 4300A and TSA MD 1400 series security policy documents and are based on the NIST 800-53 Special Publication (SP) standards. (See Section 1.4.2)

The Contractor shall include this prospective clause in all subcontracts at any tier where the subcontractor may have access to "sensitive information" as defined in this prospective clause.

4.7 General Security Responsibilities for Task Order Performance

The Contractor shall ensure that its employees follow all policies and procedures governing physical, environmental, and information security described in the various TSA regulations pertaining thereto, good business practices, and the specifications, directives, and manuals for conducting work to generate the products as required by this task order. Personnel will be responsible for the physical security of

their area and government furnished equipment (GFE) issued to them under the provisions of the task order.

All Contractor employees shall receive initial TSA IT Security Awareness Training within 60 days of assignment to the task order.

Refresher training must be completed annually thereafter.

4.8 Configuration Management (hardware/software)

Hardware or software configuration changes shall be in accordance with TSA's Configuration Management policy. The TSA Chief Information Security Officer (CISO)/ Information Assurance and Cyber Security Division (IAD) must be informed of and involved in all configuration changes to the TSA IT environment including systems, software, infrastructure architecture, infrastructure assets, and end user assets. The TSA IAD will approve any request for change prior to any development activity occurring for that change and will define the security requirements for the requested change.

4.8.1 The Contractor shall ensure all application or configuration patches and/or Request for Change (RFC) have approval by the Technical Discussion Forum (TDF), and Systems Configuration Control Board (SCCB) and lab regression testing prior to controlled change release under the security policy document, TSA Management Directive (MD) 1400.3 and TSA IT Security Policy Handbook, unless immediate risk requires immediate intervention. Approval for immediate intervention (emergency change) requires approval of the TSA CISO, SCCB co-chairs, and the appropriate Operations Manager, at a minimum.

4.8.2 The Contractor shall ensure all sites impacted by patching are compliant within 14 days of change approval and release.

4.8.3 The acquisition of commercial-off-the-shelf (COTS) Information Assurance (IA) and IA-enabled IT products (to be used on systems entering, processing, storing, displaying, or transmitting "sensitive information") shall be limited to those products that have been evaluated and validated, as appropriate, in accordance with the following:

4.8.3.1 The NIST FIPS validation program.

4.8.3.2 The National Security Agency (NSA)/National Institute of Standards and Technology (NIST) National Information Assurance Partnership (NIAP) Evaluation and Validation Program.

4.8.3.3 The International Common Criteria for Information Security Technology Evaluation Mutual Recognition Agreement.

4.8.4 Federal Desktop Core Configuration

4.8.4.1 The provider of information technology shall certify applications are fully functional and operate correctly as intended on systems using the Federal Desktop Core Configuration (FDCC) in accordance with DHS and TSA guidance. This includes Internet Explorer 7 configured to operate on Windows XP or later version and Vista (in Protected Mode on Vista). For the Windows XP settings, see:

http://csrc.nist.gov/itsec/guidance_WinXP.html, and for the Windows Vista settings, see: http://csrc.nist.gov/itsec/guidance_vista.html.

4.8.4.2 The standard installation, operation, maintenance, updates and/or patching of software shall not alter the configuration settings from the approved FDCC configuration. The information technology should also use the Windows Installer Service for installation to the default "program files" directory and should be able to silently install and uninstall.

4.8.4.3 Applications designed for normal end users shall run in the standard user context without elevated system administration privileges.

4.8.5 The Contractor shall establish processes and procedures for continuous monitoring of Contractor systems that contain TSA data by ensuring all such devices are monitored by, and report to, the TSA Security Operations Center (SOC).

4.9 Certification and Accreditation

Certification and Accreditation (C&A) in accordance with NIST SP 800-37 (current version) is a requirement for all TSA IT systems, including general support systems (e.g., standard TSA desktop, general network infrastructure, electronic mail, etc.), major applications and development systems (if connected to the operational network or processing, storing, or transmitting government data).

A written authority to operate (ATO) granted by the TSA Authorizing Official (AO) is required prior to processing operational data or connecting to any TSA network.

TSA will assign a security category to each IT system compliant with the requirements of Federal Information Processing Standards (FIPS) 199 and assign security controls to those systems consistent with FIPS 200.

Unless the AO specifically states otherwise for an individual system, the duration of any Accreditation will be dependent on the FIPS 199 rating and overall residual risk of the system; the length can span up to 36 months.

The Security Certification Package contains documentation required for C&A. The package will contain the following security documentation: 1) Security Assessment Report (SAR) 2) System Security Plan (SSP) or System Security Authorization Agreement (SSAA), 3) Contingency Plan, 4) Contingency Plan Test Results, 5) Federal Information Processing Standards (FIPS) 199 Categorization, 6) Privacy Threshold Analysis (PTA), 7) E-Authentication, 8) Security Test and Evaluation (ST&E) Plan, 9)Authorization to Operate (ATO) Letter, 10) Plan of Action and Milestones (POA&M), and 11) Annual Self-Assessments. The C&A package shall document the specific procedures, training, and accountability measures in place for systems that process personally identifiable information (PII). All security compliance documents will be reviewed and approved by the Chief Information Security Officer (CISO) and the Information Assurance and Cyber Security Division (IAD), and accepted by the Contracting Officer upon creation and after any subsequent changes, before they go into effect.

4.10 Information Technology Security Performance

The Contractor shall comply with requests to be audited and provide responses within three business days to requests for data, information, and analysis from the TSA Information Assurance and Cyber Security Division (IAD) and management, as directed by the Contracting Officer.

The Contractor shall provide support during the Information Assurance and Cyber Security Division (IAD) audit activities and efforts. These audit activities may include, but are not limited to the following: requests for system access for penetration testing, vulnerability scanning, incident response and forensic review.

4.11 Security Policy and Architecture

All services, hardware and/or software provided under this task order must be compliant with DHS 4300A DHS Sensitive System Policy Directive, DHS 4300A Sensitive Systems Handbook., TSA MD 1400.3 Information Technology Security Policy, TSA IT Security Policy Handbook and Technical Standards.

The Contractor solution shall follow all current versions of TSA and DHS policies, procedures, guidelines, and standards, which will be provided by the Contracting Officer, including but not limited to:

- DHS Sensitive Systems Policy Directive (PD) 4300A
- DHS 4300A Sensitive Systems Handbook*
- DHS National Security Systems Policy Directive (PD) 4300B
- DHS 4300B National Security Systems Handbook
- TSA MD 1400.3 Information Technology Security*
- TSA IT Security Policy Handbook
- TSA Technical Standards
- DHS IT Security Architecture Guidance Volumes 1, 2 and 3
- DHS/TSA System Engineering Lifecycle (SELC)
- DHS Performance Plan (current fiscal year)

Authorized use of TSA IT systems and resources shall be in accordance with the TSA Information Security Policy Handbook.

*See section 1.4.2

4.12 Data Stored/Processed at Contractor Site

Unless otherwise directed by TSA, any storage of data must be contained within the resources allocated by the Contractor to support TSA and may not be on systems that are shared with other commercial or government clients.

The Contractor remote access connection to TSA networks may be terminated for unauthorized use, at the sole discretion of TSA. **4.13 SBU Data Privacy and Protection**

The Contractor must satisfy requirements to work with and safeguard Sensitive Security Information (SSI), and Personally Identifiable Information (PII). All support personnel must understand and

rigorously follow DHS and TSA requirements, policies, and procedures for safeguarding SSI and PII. Contractor personnel will be required to complete online training for SSI and Informational Security, which take one hour each, as well as TSA online Privacy training.

The Contractor shall be responsible for the security of i) all data that is generated by the contractor on behalf of the TSA, ii) TSA data transmitted by the contractor, and iii) TSA data otherwise stored or processed by the contractor regardless of who owns or controls the underlying systems while that data is under the contractor's control.

TSA will identify IT systems transmitting unclassified/SSI information that will require protection based on a risk assessment. If encryption is required, the following methods are acceptable for encrypting sensitive information:

1. FIPS 197 (Advanced Encryption Standard (AES)) 256 algorithm and cryptographic modules that have been validated under FIPS 140-2. (current version)
2. National Security Agency (NSA) Type 2 or Type 1 encryption. (current version)
3. Public Key Infrastructure (PKI) (see paragraph 5.5.2 of the Department of Homeland Security (DHS) 4300A Sensitive Systems Handbook). (current version)

The Contractor shall maintain data control according to the TSA security level of the data. Data separation shall include the use of discretionary access control methods, VPN encryption methods, data aggregation controls, data tagging, media marking, backup actions, and data disaster planning and recovery. Contractors handling PII must comply with TSA MD 3700.4, *Handling Sensitive Personally Identifiable Information* (current version).

Users of TSA IT assets shall adhere to all system security requirements to ensure the confidentiality, integrity, availability, and non-repudiation of information under their control. All users accessing TSA IT assets are expected to actively apply the practices specified in the TSA Information Technology Security Policy (ITSP) Handbook and applicable IT Security Technical Standards.

The Contractor shall comply with all data disposition requirements stated in the TSA IT Security Policy Handbook, applicable Technical Standards and TSA MD 3700.4, *Handling Sensitive Personally Identifiable Information.*

4.14 Disposition of Government Resources

At the expiration of the task order, the contractor shall return all TSA information and IT resources provided to the contractor during the task order, and provide a certification that all assets containing or used to process TSA information have been sanitized in accordance with the TSA MD 1400.3, TSA IT Security Policy Handbook and Technical Standards. Proof of sanitization shall be emailed to the COTR. In addition, the contractor shall provide a master asset inventory list that reflects all assets, government furnished equipment (GFE) or non-GFE that were used to process TSA information.

4.15 Data and Data Pertinent Information (DHS Enterprise Data Management Data Modeling Methodology Guidelines)

In addition to the Federal Acquisitions Regulations (FAR) Subpart 27.4 – 'Rights in Data and Copyrights' and Section 35.011 detailing technical data delivery, the contractor shall provide all TSA-specific data in a format maintaining pre-existing referential integrity and data constraints, as well as data structures in an understandable format to TSA. Examples of data structures can be defined as, but not limited to:

- Data models depicting entity relationships
- Metadata information to define data definitions
- Detailed data formats, type, and size
- Delineations of the referential integrity (primary key/foreign key) of data schemas

All TSA-specific data shall be delivered in a secure and timely manner to TSA. Data security is defined within Section VII, 'Requirements for Handling Sensitive, Classified, and/or Proprietary Information,' within this SOW. This definition complies with not only the delivery of data, but also maintaining TSA-specific data within a non-TSA or DHS proprietary system. Alternative data delivery techniques may also be defined by TSA EDM project team.

As part of the necessary data structure, the contractor shall provide an Entity Relationship Diagram (ERD) to explain the business relationships to TSA through graphically and textually detailing the data that is stored per each database and system/application, or any data provided via a service. The preferred format for the ERD is CA Erwin; however other formats, such as Visio, DLL, database scripts or format specified by TSA EDM project team shall be accepted. All additional known data models (e.g., Logical Data Model (LDM) Conceptual Data Model (CDM), Physical Data Model (PDM), Data Flow Diagrams (DFD)) depicting TSA-specific data are required. Referential integrity also needs to be addressed for all parent/child or primary key/foreign key relationships within these models.

All metadata shall be pre-defined upon delivery to TSA. Metadata shall be delivered in a format that is readily interpretable by TSA (e.g. metadata shall be extracted from any metadata repository that is not utilized by TSA and delivered in a TSA approved manner). Metadata shall also provide an indication of historical verses the most current data to be used, as well as frequency of data refreshes.

The contractor shall adhere to providing a Data Management Plan (DMP), as defined by the TSA Enterprise Data Management (EDM) project team, which includes conceptual and logical data models, along with a data asset profile. Any data exchanges with other DHS Components shall adhere to DHS data exchange standards using the National Information Exchange Model (NIEM). All required artifacts will be provided to the TSA EDM project team for their review and approval. The contractor shall use the attached DMP template.

Note: The following definitions pertain to the previous paragraphs:

An ERD is a diagram used to identify the topics of interest (entities) and their connections to each other (relationships).

An LDM in systems engineering is a representation of an organization's data, organized in terms of entities and relationships and is independent of any particular data management technology.

'A CDM is a high-level model that is considered a useful first step in documenting and describing the fundamental nature of the organization's data. It serves as the foundation for providing a common vocabulary and for understanding the overall structure of data, and for normalizing data access to support improved information sharing. In a CDM, fundamental things of significance to the business

organization are represented. A CDM usually includes data objects and the corresponding core relationships in terms of the business user.

A PDM is a representation of a data asset design which takes into account the facilities and constraints of a given ***database management system*** *(DBMS). It is typically derived from a logical data model, though it may be reverse-engineered from a given database implementation. The PDM can usually be used to calculate storage estimates and may include specific storage allocation details for a given database system. There is no sharp dividing line between a CDM and an LDM. Similarly, there is no sharp dividing line between an LDM and a PDM. Depending on the developers and their requirements, details may appear in one model or the other. Each model should be constructed down to the level of detail that makes the model useful to the intended audience.'*[1]

A DFD is a diagram depicting the flow of data from the source to the target systems, showing all interactions made in between.

Referential integrity is a database concept that ensures that relationships between tables remain consistent. When one table has a foreign key to another table, the concept of referential integrity states that you may not add a record to the table that contains the foreign key unless there is a corresponding record in the linked table.

5.0 GOVERNMENT TERMS AND DEFINITIONS

5.1 SHARE: Safety, Health and Return-to-Work Initiative

5.2 DHS: Department of Homeland Security

5.3 POWER: Protecting Our Workers and Ensuring Reemployment Initiative

5.4 TSA: Transportation Security Administration

5.5 WCP: Workers' Compensation Program

5.6 TSOs: Transportation Security Officers

5.7 MCM: Medical Case Management or Medical Case Manager

5.8 FROI: First Report of Injury

5.9 IT: Information Technology

5.10 SOW: Statement Of Work

[1] These definitions have been defined through the 'DHS Enterprise Data Management – Data Modeling Methodology Guidelines' found on the DHS Connect DMWG Portal which can be found at http://dhsconnect.dhs.gov/org/comp/mgmt/cio/aot/Pages/DataManagementWorkingGroup.aspx

5.11 ATSA: Aviation and Transportation Security Act

5.12 FECA: Federal Employees Compensation Act

5.13 OWCP: Office of Workers' Compensation Programs

5.14 MD: Management Directive

5.15 SDLC: Systems Deployment Life Cycle

5.16 SLC: Systems Life Cycle

5.17 USC: United States Code

5.18 CFR: Code of Federal Regulations

5.19 ITSP: Information Technology Security Policy

5.20 SSI: Sensitive Security Information

5.21 FISMA: Federal Information Security Management

5.22 DOL: Department Of Labor

5.23 C&A: Certification and Accreditation

5.24 RN: Registered Nurse

5.25 WCC: Workers' Compensation Coordinator

5.26 PBM: Pharmacy Benefits Management Network

5.27 COOP: Continuity of Operations Plan

5.28 MRP: Medical Review Physician

5.29 EDD: Estimated Disability Duration

5.30 MDA: Medical Disability Advisor

5.31 PR: Periodic Roll

5.32 OHC: Office of Human Capital

5.32 COTR: Contracting Officer Technical Representation

5.33 BCP: Business Continuity Plan

5.34 EIT: Electric and Information Technology

5.35 GOTS Government Off-the-Shelf

5:36 COTS: Commercial-Off-The-Shelf

5.37 AJAX: Asynchronous Javascript and XML

5:38 OAST: DHS Office of Accessible Systems and Technology

5.39 HLS EA: Homeland Security Enterprise Architecture

5.40 TRM: Technical Reference Model

5.41 EDMO: DHS Enterprise Data Management Office

5.42 OMB: Office of Management and Budget

5.43 DMP: Data Management Plan

5.44 EAD: Enterprise Architecture Division

5.45 SER: Solution Engineering Review

5.46 PDR: Preliminary Design Review

5.47 CDR: Critical Design Review

5.48 FRD Functional Requirements Document

5.49 SDD: System Design Document

5.50 SSP: System Security Plan

5.51 PCII: Protected Critical Infrastructure Information

5.52 GFE: Government Furnished Equipment

5.53 CSO: Chief Security Officer

5.54 CIO: Chief Information Officer

5.55 NDA: Non-Disclosure Agreement

5.56 SP: Special Publication

5.57 CISO: Chief Information Security Officer

5.58 IAD: Information Assurance and Cyber Security

5.59 RFC: Request for Change

5.60 SCCB: Systems Configuration Control Board

5.61 NSA: National Security Agency

5.62 NIST: National Institute of Standards and Technology

5.63 TDF: Technical Discussion Forum

5.63 NIAP: National Information Assurance Partnership

5.63 FDCC: Federal Desktop Core Configuration

5.64 SOC: TSA Security Operations Center

5.65 ATO: Authority To Operate

5:66 AO: Authorizing Official

5.67 FIPS: Federal Information Processing Standard

5.68 SSAA: System Security Authorization Agreement

5.69 PTA: Privacy Threshold Analysis

5.70 POAM: Plan Of Action and Milestones

5.71 CISO: Chief Information Security Officer

5.72 AES: Advanced Encryption Standard

5.73 PKI: Public Key Infrastructure

5.74 ITSP: Information Technology Security Policy

5.75 DRE: Durable Medical Equipment

5.76 GSA: General Services Administration

5.77 GSA FTR: General Services Administration Federal Travel Regulations

5.78 CLIN: Contracting Line Item Number

5.79 CO: Contracting Officer

5.80 MRPD: Medical Review Programs Division

5.81 SSN: Social Security Number

5.82 Sensitive PII: Sensitive Personally Identifiable Information

5.83 EDM: Enterprise Data Management

5.84 ERD: Entity Relationship Diagram

5.85 LDM: Logic Data Model

5.86 CDM: Conceptual Data Management

5.87 PDM: Physical Data Management

5.88 DFD: Data Flow Diagrams

5.89 DBMS: Database Management System

5.90 DMPC: Data Management Plan Checklist

5.91 OIT: Office of Information Technology

5.92 DMWG: Data Management Working Groups

5.93 EDM: ConOps; Enterprise Data Management Concept of Operations

5.94 DRM: Data Reference Model

5.95 DMM: Data Management Maturity

5.96 DMPG: Data Management Plan Guide

5.97 RTM: Requirements Traceability Matrix

5.98 SLA: Service Level Agreement

5.99 ISSA: Information Sharing Access Agreement

5.100 NIEM: National Information Exchange Model

5.101 IEPD: Information Exchange Package Documentation

5.102 T&S: Transition and Sequencing

5.103 HQ-WCP: Headquarters Workers' Compensation Program Office

5.104 Medical Case Managers a certified/licensed Registered Nurses (RN) within the respective state(s) for which they will provide services to TSA employees.

5.105 Breach means the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar situation where persons other than authorized users,

and for other than authorized purpose, have access or potential access to Personally Identifiable Information, in usable form whether physical or electronic.

5.106 Personally Identifiable Information (PII)" means any information that permits the identity of an individual to be directly or indirectly inferred, including any other information that is linked or linkable to that individual regardless of whether the individual is a citizen of the United States, legal permanent resident, or a visitor to the United States.

5.107 Sensitive Personally Identifiable Information (Sensitive PII)" a subset of Personally Identifiable Information, which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Complete social security numbers (SSN), alien registration numbers (A-number) and biometric identifiers (such as fingerprint, voiceprint, or iris scan) are considered Sensitive PII even if they are not coupled with additional PII. Additional examples include any groupings of information that contains an individual's name or other unique identifier plus one or more of the following elements:

(1) Driver's license number, passport number, or truncated SSN (such as last 4 digits)
(2) Date of birth (month, day, and year)
(3) Citizenship or immigration status
(4) Financial information such as account numbers or Electronic Funds Transfer Information
(5) Medical Information
(6) System authentication information such as mother's maiden name, account passwords or personal identification numbers (PIN)

5.108 Data Management Plan (DMP), as defined by the TSA Enterprise Data Management project team, which includes conceptual and logical data models, along with a data asset profile

5.109 A Compact State is defined as a compact, or multi-state, license allows a licensed Registered Nurse (RN) to work in another state without having to obtain licensure in that state.

5.110 A Medical Status Report is a report containing to most recent medical status of each claim in the program. Status meaning; total disability, fit for limited duty, fit for regular duty and etc.

6.0 SPECIAL REQUIREMENTS – PERSONNEL QUALIFICATIONS (IN ADDITION TO HSAR 3052.204-71)

6.1 The Medical Case Managers (MCM) shall be certified Registered Nurses (RN) within the respective state(s)or maintain a respective Nurse Licensure Compact that enables multistate licensure to provide services to TSA employees.

NOTE: The Contractor shall provide at least one MCM that holds a valid California Nursing License.

6.2 The MCMs shall possess and maintain the required professional certification or license within

the respective state(s) necessary to provide or perform the services required.

6.3 Each MCM shall maintain a national certification in case management or a related field and have prior workers' compensation experience preferably with FECA.

6.4 The MCMs shall have knowledge and understanding of FECA, regulations and its application as it applies to federal workers compensation claims management.

6.5 The Medical Review Physician (MRP) role is a leadership position requiring regular effective interaction with headquarters, workers' compensation coordinators, nurse case managers, and treating medical providers.

6.6 The MRP shall have an active medical license in one of the 50 United States, and current board certification in Occupational Medicine.

6.7 The MRP shall have expertise in case management, with at least two years in verbal and report writing communication skills.

6.8 MRP shall have an understanding of disability prevention best practices and strategies appropriate for the federal employees.

6.9 Required MRP experience:

- At least 5 years of workers' compensation clinical care or case management required.
- At least 2 years occupational health clinic management.
- Workers' compensation or disability chart reviews and report writing.

6.10 Interface

The MCM Contractor shall provide access to ancillary networks to assist employees recovering from work related injuries. At a minimum the networks should include the following; Pharmacy Benefits Management (PBM), Radiology Diagnostic, and Durable Medical Equipment (DRE) networks.

6.11 Transition

During the transition in period, the incumbent Contractor shall be responsible for the delivery of MCM Services until the incoming Contractor has completed C&A and personnel vetting.

The incoming Contractor shall implement its Transition Plan, as approved by the Contracting Officer. The purpose of the Transition Plan is to ensure efficient, smooth, seamless and uninterrupted transition of TSA's medical case management data from the out-going Contractor to the incoming Contractor.

The Transition Plan shall detail all information required by the incoming Contractor from both the outgoing Contractor and TSA. As a minimum, details shall include all processes required to transition and migration from the outgoing to the incoming Contractor. The Plan shall provide the identification of

all necessary tasks and objectives, including the relocation of all files and records, milestones, planned staffing levels, provisions for written progress reports, to include system notes, and in-process reviews. The incoming Contractor shall be capable of receiving, storing and maintaining a historical database of all TSA's workers' compensation claims and case files collected; and, to transition and migrate all of the existing TSA historical data files to a centralized database system.

Therefore the incoming system must have the capability to import cases, tables, and other data from the current MCM system to maintain continuity of operations. TSA will provide the incoming MCM Services Contractor with the necessary equipment and information to access the existing web-based medical management IT system. The incoming MCM Service Contractor's system shall interface with the TSA provided equipment. The incoming MCM Services Contractor shall conduct medical case management database training for its medical case managers to stay abreast of database changes. The incoming MCM Service Contractor shall provide all System Training for TSA users.

During the transition out period, at the conclusion of task order performance, the Contractor shall turn over all records as directed by TSA and cooperate with a new Contractor, if required. The Contractor shall provide on-going litigation support with respect to claims filed during the task order period of performance.

7. DELIVERABLES

#	Deliverable	Frequency*	Due Date*	Deliverable Recipient include contact information	Deliverable Format**	Linkage to Technical Requirements
1.	Draft Project Plan	N/A	10 Days After Award	COTR	Microsoft Word and/or Excel	Section 4.0
2.	Final Project Plan	N/A	30 Days After acceptance of draft	COTR	Microsoft Word and/or Excel	Section 4.1
3.	Transition Plan	N/A	30 Days After Award	COTR	Microsoft Word and/or Excel	Section 6.11

4.	Business Continuity Plan	30 Days After Award	30 Days After Award	COTR	Microsoft Word and/or Excel	Section 4.2
5.	Program Status Report	Daily, Weekly, Monthly, Quarterly, Semi-annual, Annual	First one due 10 days after Task order Award	WCP PM, COTR	Microsoft Excel	Task 4 - Section 2.4.3
6.	Quality Assurance Report	Annual	30 day after most recent period of performance ends	WCP PM and COTR	Microsoft Word	Task 4 - Section 2.4.4
7.	Customer Satisfaction Monitoring Tool	Quarterly	To be delivered at program status meetings	HQ-WCP Staff and COTR	Word and/or Excel	Task 4 - Section 2.4.5
8.	WCP Quality, Improvement Recommendations Report	As needed	To be presented at program status meetings	HQ-WCP Staff and COTR	Microsoft Word	Task 4 – Section 2.4.6
9.	Operational Performance Report (MCM Responsiveness and Effectiveness)	Bi-weekly	To be delivered at program status meetings	HQ-WCP Staff and COTR	Microsoft Word, Excel, PowerPoint	Task 4 – Section 2.4.7
10.	WCP Improvement Recommendation Assessment	As needed	To be presented at program	HQ-WCP Staff and COTR	Word, Excel, PowerPoint	Task 4 – Section 2.4.10

	Process Report		status meetings			
11.	Data Management Plan (DMP)	60 days from start of MCM services	60 days from start of MCM services	OIT and COTR	Microsoft Word	Section 4.4

***Calendar days**

**** See Section V.2 for software versions**

8. PERIOD OF PERFORMANCE

The period of performance is one twelve month base period with four (4) one year option periods. The contract effective date will commence after vetting of personnel. Upon completion of Certification and Accreditation the IT Solution portion of the task order will commence. The duration of any awarded task order must be in sync with the awardee's GSA Schedule contract.

9. TRAVEL/OTHER DIRECT COST (ODC) REQUIREMENTS

Travel may be required under this task order. All travel associated with Government business as a result of this task order should follow GSA Federal Travel Regulations (GSA FTR) and can be viewed at www.gsa.gov. Travel should be coordinated and approved in advanced by the HQ-WCP Program Manager, Contracting Officer or COTR. A separate contracting line item number (CLIN) will be assigned for travel costs on a cost reimbursable basis. All travel shall be scheduled sufficiently in advance to take advantage of offered discount rates, unless the HQ-WCP Program Manager authorized other arrangements. Local travel costs will not be reimbursed. The Contractor will be required to submit receipts for all related travel costs equal to or in excess of $25.00.

The other direct costs may include office supplies, postage, shipping and handling, and other miscellaneous items as required in support of the subject task order.

10. GOVERNMENT FURNISHED RESOURCES AND INFORMATION

The Contractor will be provided with government furnished equipment as identified below:

The Contractor, on behalf of the Government, shall purchase printers with fax and scanning capability, and cellular phones. These items shall be purchased as ODCs under the subject task order. Upon purchase, the Contractor shall immediately transfer ownership to the Government at which time the Government will inventory all equipment and issue to the Contractor as Government Furnished Property. All laptops will be purchased by the Government for the contractor and supplied as Government Furnished Property.

After the end of the task order, the Contractor shall provide a certification that all equipment contained or used to process TSA information has been sanitized in accordance with TSA requirements (section 4.14) and deliver laptops containing both sensitive and non-sensitive information and a complete inventory list to the Worker Compensation Program Management Office and COTR for approval. The Contractor shall ship to the TSA Equipment Warehouse via a TSA approved method of shipping.

The Contractor shall not connect its privately owned portable computers to the TSA local area network, nor use TSA's voice over internet protocol telephone system to connect portable computers to its home office.

PROGRAM MANAGEMENT OFFICE

Transportation Security Administration (TSA)
Worker's Compensation Program Office
POC: Darryl Thornton

REQUIRING ORGANIZATION

Department of Homeland Security
Transportation Security Administration (TSA)
Office of Human Capital
Medical Review Programs Division (MRPD)
Worker's Compensation Program Office
TSA 21
601/701 South 12th Street
Arlington, Virginia 20598-6021